RECEIVED
CENTRAL FAX CENTER
JAN 18 2007

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims

1. (currently amended) A method of authenticating a host to receive content from a media player, the method comprising:

receiving at the media player a certificate from the host, the certificate including a plurality of fields, including a field holding a digital signature from a certifying authority;

verifying the digital signatures in the certificate, the verifying including at least one of:

verifying the certifying authority digital signature using the certifying authority public key; ~~and~~

verifying a host digital signature using a host public key; ~~and~~

receiving validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria;

if the digital signatures are verified and validated, generating a random number at the media player to form a session key and encrypting the session key with a public key extracted from the certificate to form an encrypted session key and transmitting the encrypted session key to the host;

at the host, receiving an encrypted content key from the media player;

decrypting the encrypted content key using the session key to recover the content key;

at the media player, retrieving encrypted content from a media;

transmitting the encrypted content to the host; and

at the host, decrypting the encrypted content using the content key.

2. (Original) The method of claim 1 wherein the source is one of a portable medium and firmware.

3. (Cancelled)

4. (Cancelled)

5. (Previously Presented) The method of claim 1 wherein the certifying of the host includes certifying a second host for a host to second host secure communication channel, the certifying allowing a copy function between the host and the second host.

6. (Previously Presented) The method of claim 1 wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the host.

7. (Previously Presented) The method of claim 6 wherein the source validation data is compared with the data in the certificate to identify as invalid one or more of the product category, the product line, the model, the revision and the serial number of the host.

8. (Previously Presented) The method of claim 1 wherein the certificate includes one or more of a certifying authority identifier field, a version field, a sign key identifier field, an exposed methods field, a company field, a model identifier field, a revision field, a metadata identifier field, a device digital signature key field, a certifying authority digital signature field, a serial number field, a protocol public key field and a device digital signature field, wherein the

certifying authority digital signature verifies one or more of the fields in the certificate and the host digital signature verifies one or more of the fields in the certificate.

9. (Previously Presented) The method of claim 1 wherein the certificate enables an entity receiving the certificate to control the quality of the host by invalidating hosts that are false or have latent defects.

10. (Previously Presented) The method of claim 6 wherein the certificate further includes fields provided by a host manufacturer, including the company public key, wherein the company public key is digitally signed by the certifying authority.

11. (Previously Presented) The method of claim 6 wherein the certificate further includes fields provided by a host manufacturer, the fields including the host public key, wherein the host public key is digitally signed by the company.

12. (Previously Presented) The method of claim 6 wherein one or more of the product category, the product line, the model, the revision and the serial number of the host are provided to a certificate creator after the host passes a qualification procedure.

13. (Original) The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key.

14. (Previously Presented) The method of claim 13 wherein the set of methods includes digital rights management (DRM) methods include one or more of a copy method, a record

method, a play method, a read secure metadata method, a write secure metadata method, and an unlock method, the DRM methods operable according to a type of the host.

15. (Cancelled)

16. (Original) The method of claim 1 wherein each of the fields hold 326-bit values for 163-bit elliptic curve cryptography.

17. (Original) The method of claim 1 wherein the certifying authority public key is referenced by a field of the certificate.

18. (previously presented) The method of claim 1 wherein the certifying authority public key is in a firmware component.

19. (Cancelled)

20. (currently amended) A media player configured to certify a host, the media player comprising:

a firmware component including:

a block configured to receive a certificate from the host, the certificate including a plurality of fields, including a field holding a protocol public key;

a block configured to verify one or more digital signatures in the certificate, including at least one of:

a certifying authority digital signature using a certifying authority public key; and

a device digital signature using a device public key in the certificate; ~~and~~

a block configured to receive validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria;

a block configured to generate a random number and transmit the random number to the host if the digital signatures are verified and validated; and

a block to transmit an encrypted content key to the host, wherein the host is enabled to recover a content key from the encrypted content key by using the random number, the media player being operable to retrieve encrypted content from a media and provide the encrypted content to the host such that the host is enabled to decrypt the encrypted content using the content key.

Claims 21-23. (cancelled)